医療業界で増加し続ける ランサムウェア攻撃の対策とは

二要素認証・アクセス制御で不正アクセスを防ぐ　UserLock

医療機関に求められるランサムウェア対策

近年ランサムウェア攻撃が増加し続けており、企業や組織はその対応に追われています。もともとランサムウェア攻撃はWebページやランダムメールなどで無差別的に攻撃を仕掛ける手法でしたが、最新型のランサムウェア攻撃では特定の企業や組織を狙う標的型の攻撃に変わっており、ネットワークに侵入後、**ラテラルムーブメント(横方向への移動)**でより権限のある管理者アカウントを狙います。そしてデータの暗号化を行い、解除のための身代金を要求する流れになっています。特に**カルテなどの重要な個人情報を扱う医療機関**は標的として狙われやすくなっています。

ランサムウェア被害が起こった場合考えられるリスク

■長期間の診療停止(電子カルテシステムや会計システム停止など)
■システム再構築による多額の費用支出(実例:2億円)
■多額の身代金支払いによる損失　など

実例として、関連先等のセキュリティ対策に脆弱性のある企業や組織のアカウント情報を取得し、**不正アクセスを行い**、なりすましからランサムウェアに感染させるケースが多くなっており、関係企業含めてシステムや**ネットワーク内部**のセキュリティ対策が重要です。
UTMやエンドポイントセキュリティなどネットワークの外部を守るツールはありますが、**ネットワークの内部**はどうでしょうか？既存の**ID・パスワードだけでは、なりすましによる不正アクセス**を防ぐことは難しいと言わざるを得ません。

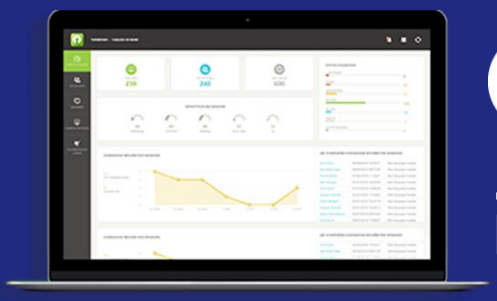
対策ポイントは二要素認証

医療情報システムの安全管理に関するガイドライン 6.0版

※システム運用編　14. 認証・認可に関する安全管理措置の遵守事項より抜粋

利用者認証にパスワードを用いる場合には、令和9年度時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新するに際しては、**二要素認証**を採用するシステムの導入、又はこれに相当する対応を行うこと。

「二要素認証」の実装の優先度が高くなっています！



UserLock®

二要素認証・柔軟なアクセス制御で不正アクセスを防ぎ、ネットワーク内部で起こるリスクを抑止

二要素認証＋同時ログイン制御によるなりすまし対策

UserLockは二要素認証を簡単に導入、アプリケーションだけでなくハードウェアトークンなどにも対応。また同一アカウントによる同時ログインの制御が可能です。

- ●職員間のアカウント不正利用を防ぐ
- ●不正利用検知時にシステム管理者だけでなく、職員自身にもアラートを通知
- ●二要素認証の要求頻度の設定が可能なため、時間がない医療従事者向けに業務効率を下げずに対応可能

クローズドネットワークにおけるアクセス制御

UserLockは原則インターネット接続が許可されていないようなクローズドネットワークにおいても二要素認証やアクセス制御機能を提供します。

- ●完全オンプレミス型のアクセス制御により隔離されたクローズド環境にも対応
- ●カルテなどの高度な機密情報を扱うネットワークへのセキュアなアクセスに有用
- ●インターネット接続が前提のクラウド型のIDaaSでは対応不可

踏み台サーバーを運用したシステムのセキュリティ強化

UserLockはサプライチェーンの共有ネットワーク・共有サーバーへの二要素認証、時間外ログインの制御、アクセス状況の可視化を提供します。

- ●踏み台サーバーだけでなく、接続先のサーバーも保護
- ●アクセス状況のリアルタイム監視、疑わしいアクセスに対してはアラートを通知
- ●深夜・休日などの業務時間外の原則アクセス不可といった対応も可能

OCEANBRIDGE
株式会社オーシャンブリッジ
〒107-0051 東京都港区元赤坂1-5-12 住友不動産元赤坂ビル7F
Web：https://www.isdecisions.jp/
Mail：userlock@oceanbridge.jp